Contents

Abstract **11**

1 Introduction **13**
1.1 Motivation 13
1.2 Contribution 15
1.3 Structure 17

2 Pervasive Computing Concepts **19**
2.1 Pervasive Computing 19
2.1.1 Context 20
2.1.2 Roles 23
2.1.3 System-support for Pervasive Computing 26
2.1.4 Devices 28
2.2 Security Goals 30
2.2.1 Confidentiality 30
2.2.2 Integrity 31
2.2.3 Availability 31
2.2.4 Authenticity 32
2.2.5 Privacy 33
2.3 Applications 34
2.3.1 PECES 34
2.3.2 GAMBAS 36

3 System Support for Security and Privacy in Pervasive Computing **39**
3.1 Related Work 39
3.1.1 Type of Pervasive Infrastructure 39
3.1.2 Environment Boundaries 41
3.1.3 Context and Role Privacy and Security 43
3.1.4 Trust 44
3.1.5 Secure Key-exchange 46
3.1.6 Individual Privacy Policy 48
3.2 Requirements for Security and Privacy in Pervasive Computing 50

4 Peer-based Context Management 55

4.1 Privacy-Preserving Context Management 55
4.1.1 Preliminaries 55
4.1.2 Context Model 56
4.1.3 System Architecture 58
4.2 Secure Context Distribution Framework 61
4.2.1 Preliminaries 61
4.2.2 System Model 63
4.2.3 Example Scenario 63
4.2.4 Requirements 64
4.2.5 Context Distribution Framework 65
4.3 Conclusion 71

5 Secure Adaptation with Role Assignment 73

5.1 Preliminaries 73
5.2 Requirements 75
5.3 Approach 76
5.3.1 Generic Role Assignment 77
5.3.2 Adaptive Environment Role Assignment 78
5.3.3 Secure Role Assignment 79
5.3.4 Trust Model 80
5.3.5 Security Rules 81
5.3.6 Security Enforcement 83
5.4 Implementation 85
5.4.1 Architecture 85
5.4.2 Interaction 88
5.4.3 Integration 91
5.5 Applications 94
5.5.1 Traffic Management 95
5.5.2 E-Health 96
5.6 Conclusion 97

6 Secure Key-Exchange 99

6.1 Preliminaries 99
6.2 Approach 101
6.2.1 System Model and Assumptions 101
6.2.2 Design Rationale and Goals 102
6.2.3 Key Exchange Protocol 103
6.3 Implementation 110
6.3.1 Core Library 110
6.3.2 Google Calendar Plug-in 111
6.3.3 Facebook Event Plug-in 112

6.4 Applications . . . 113
6.4.1 Privacy-preserving Speaker Recognition . . . 114
6.4.2 Configuration-free Conference Registration . . . 115
6.4.3 Energy-efficient Resource Sharing . . . 115
6.5 Conclusion . . . 117

7 Automating Policy Generation 119
7.1 Preliminaries . . . 119
7.2 Approach . . . 120
7.2.1 System Model . . . 121
7.2.2 Design Rationale and Goals . . . 122
7.2.3 Privacy Policy Generation Framework . . . 123
7.3 Implementation . . . 126
7.3.1 Context Types and Recognition . . . 126
7.3.2 Privacy Policy Generator Library . . . 127
7.3.3 Google Calendar Plug-in . . . 130
7.3.4 Facebook Status Messages Plug-in . . . 130
7.4 Application . . . 131
7.5 Conclusion . . . 133

8 Evaluation 135
8.1 Privacy-Preserving Context Management . . . 135
8.1.1 Experiments . . . 136
8.1.2 Qualitative Evaluation . . . 139
8.2 Secure Context Distribution Framework . . . 140
8.2.1 Discussion . . . 140
8.2.2 Measurements . . . 141
8.2.3 Qualitative Evaluation . . . 144
8.3 Secure Adaptation with Role Assignment . . . 144
8.3.1 Configurable . . . 145
8.3.2 Composable . . . 146
8.3.3 Flexible . . . 146
8.3.4 Secure . . . 147
8.3.5 Light-weight . . . 148
8.3.6 Experiments . . . 148
8.3.7 Qualitative Evaluation . . . 154
8.4 Secure Key-Exchange . . . 156
8.4.1 Full Automation . . . 156
8.4.2 High Security . . . 156
8.4.3 Low Latency . . . 158
8.4.4 Scalability . . . 161
8.4.5 Qualitative Evaluation . . . 162

8.5 Automating Policy Generation 164
8.5.1 Generic 164
8.5.2 Extensible 165
8.5.3 Automation 166
8.5.4 Low Overhead 166
8.5.5 Qualitative Evaluation 169
8.6 Conclusion 169

9 Conclusions and Outlook 173
9.1 Outlook 175

Bibliography 177